IMAGE COMPRESSSION AND ENCRYPTION USING SCAN PATTERN

A Thesis Submitted in Partial Fulfillment
of the Requirements for the Award of the Degree of

Master of Technology
In
Communication and Network Engineering

submitted by
Mr. SNEHASHIS JHA
Roll no.212EC5172

DEPARTMENT OF ELECTRONICS AND COMMUNICATION
NIT ROURKELA
ROURKELA-769008

IMAGE COMPRESSSION AND ENCRYPTION USING SCAN PATTERN

A Thesis Submitted in Partial Fulfillment
of the Requirements for the Award of the Degree of

Master of Technology
In
Communication and Network Engineering

submitted by
Mr. SNEHASHIS JHA
Roll no.212EC5172

under the guidance of
Prof. SUKADEV MEHER
Dept. of ECE
NIT Rourkela

DEPARTMENT OF ELECTRONICS AND COMMUNICATION
NIT ROURKELA
ROURKELA-769008

CERTIFICATE

This is to certify that the Thesis Report entitled **"IMAGE COMPRESSION AND ENCRYPTION USING SCAN PATTERN"** submitted by **SNEHASHIS JHA** bearing roll no. **212EC5172** in partial fulfillment of the requirements for the award of Master of Technology in Electronics and Communication Engineering with specialization in **"COMMUNICATION AND NETWORKS"** during session 2012-2014 at National Institute of Technology, Rourkela is an authentic work carried out by him under my supervision and guidance.

Prof. Sukadev Meher
Head of the Department
Department of ECE
National Institute of Technology
Rourkela-769008

Date:

ACKNOWLEDGEMENTS

First of all, I would like to express my deep sense of respect and gratitude towards my advisor and guide **Prof. S. Meher**, who has been the guiding force behind this work. I am greatly indebted to him for his constant encouragement, invaluable advice and for propelling me further in every aspect of my academic life. His presence and optimism have provided an invaluable influence on my career and outlook for the future. I consider it my good fortune to have got an opportunity to work with such a wonderful person.

Next, I want to express my respects to all the professors in my department for teaching me and also helping me how to learn. They have been great sources of inspiration to me and I thank them from the bottom of my heart.

I also extend my thanks to all faculty members and staff of the Department of Electronics and Communication Engineering, who have encouraged me throughout the course of Master's Degree.

I would like to thank all my friends and classmates for all the thoughtful and mind stimulating discussions we had, which prompted us to think beyond the obvious.

I am especially indebted to my parents for their love, sacrifice, and support. They are my first teachers after I came to this world and have set great examples for me about how to live, study, and work.

TABLE OF CONTENTS

TITLE……PAGES

TITLE……PAGES

LIST OF FIGURES

TITLE……PAGES

LIST OF TABLES

TITLE……PAGES

ABSTRACT

The methodology of image compression and encryption using scan pattern is an algorithm which is capable of doing both compression and encryption of an image simultaneously. It is a method applied on binary images. The methodology is applied on grayscale sample images, by dividing the grayscale image into its corresponding bit planes. The main aim of the algorithm is to find a good scan path which can compress an image using least bits required. The compression is done using run-length coding. The encryption is done again using a scan path which is kept secret; this is used as the key for encryption.

Here in this work the methodology is applied on the sample image in two ways. One is done using single key encryption where there is one key to encrypt and decrypt the image. And another is double key encryption where the scan path for compression is also used as a key for encrypting and decrypting an image.

CHAPTER 1:

INTRODUCTION

INTRODUCTION

Image compression and encryption has been a great area of interest since images are being used as one of the most valuable information source in many areas like medical application, military application, space science application and many more. There are three types of image namely binary image, grayscale image and colour image. Binary image has only two intensity levels black and white, whereas grayscale images have 256 intensity levels and colour images have various colour map each of which have 256 intensity levels. For the being here the area of interest is grayscale image.

Now the first question that arises is what is image compression and encryption and why it is needed? Image compression means reducing the size of an image without or with a certain loss of data. This is needed because for an image which need to be transmitted over a channel will consume a large bandwidth according to its size. So if the size can be reduced the bandwidth needed for the transmission of the compressed image will be less. Encryption on the other hand is needed to provide security to the information. This is a method or a process for protecting information from undesirable attacks by converting it into a form non recognizable by its attackers. Data encryption mainly is the scrambling of the content of data, such as text, image, audio, video and so forth to make the data unreadable, invisible or incomprehensible during transmission. The goal is to protect the content of the data against the attackers. The reverse of data encryption is data decryption, which recovers the original data.

1.1 **IMAGE:**

An image is actually a 2-D signal processed by the human visual system[15]. Image can be of both analog and digital type. However, at the time of process, storage and transmission it has to be in the form of digital type. A digital image is nothing but a 2- D array of pixels. Image plays a key role in part of providing information, significantly in remote sensing, medical specialty and video conferencing applications. The employment of and dependence on information carrying image and its application is still growing.

1.2 IMAGE COMPRESSION

Image compression is the process of reducing the amount of information needed to represent a digital image. It is a process supposed to achieve a compact illustration of associate degree image, thereby reducing the image storage/transmission requirements[15]. Compression is done by reducing one or a lot of the 3 basic data redundancies:

1. Coding Redundancy
2. Interpixel Redundancy
3. Psychovisual Redundancy

Coding redundancy is present once when optimum code words are used. Interpixel redundancy is obtained from correlations between the pixels of a picture. Psychovisual redundancy refers to those information that's unrecognizable by the human visual system (i.e. visually non-essential information). Image compression techniques decreases the amount of bits required to represent an image by taking advantage of those redundancies. An inverse method known as decompression (decoding) is applied to the compressed image to obtain the reconstructed image. The target of compression is to reduce the amount of bits as much as possible, whereas keeping the resolution intact and therefore the visual quality of the reconstructed image as near the initial image as attainable. Image compression systems area unit composed of 2 distinct structural blocks : An encoder and a decoder.

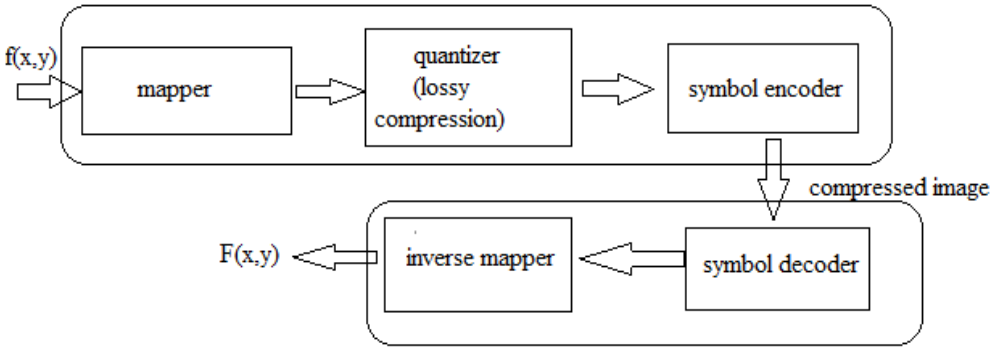


fig.1.1:basic block diagram for image compression and decompression

There are two type of compression scheme as mentioned earlier: lossless compression and lossy compression. In case of lossless compression only the statistical redundancy is exploited to achieve compression, so the compressed image is likely to be same as the original image. Data compression techniques such as LZW or LZ77 are used in .GIF, .PNG AND .TIFF file formats. Compression ratios for the techniques used are typically ~2:1 for natural imagery but can be much higher for document images. Lossy compressions on the other hand both statistical and perceptual irrelevancy of image data are exploited. So the reconstructed image contains degradation with respect to the original image. The compression ratio achieved is much higher as compared to the lossless compression. The term **visually lossless** is often used to characterize lossy compression schemes that result in no visible degradation under a set of designated viewing conditions.

1.3 IMAGE ENCRYPTION

1.3.1 CRYPTOGRAPHY

Encryption and decryption are two phases of a process called cryptography[14],[16]. Cryptography is a process of storing and transmitting data in a form that only intended person can read and process it. It is a science of protecting information by encoding it into an unreadable format. Data that can be read or understood without any special measurement is called *plaintext*. The method of rearranging the data into some unreadable form is called *encryption.* Encrypted plaintext is called *ciphertext*. The algorithm used to encrypt a plaintext is called *cypher*. An algorithm works in a combination with a *key* – a word, number, or phrase – to encrypt the data.
Based on the keys used in a cypher, there are two type of algorithm namely *Symmetric Key algorithm* and *Asymmetric Key algorithm*. In symmetric key there is a single key that is used in both ends to encrypt and decrypt a data. But in case of asymmetric key there are two keys that are used in the algorithm namely *public key* and *private key*.
Here in case of image encryption symmetric key algorithm has been used.

1.3.2 IMAGE ENCRYPTION USING SCAN PATTERNS

The proposed image encryption method is actually based on the rearrangement of the pixels of an image. The rearrangement is achieved by the scan patterns and it is also used as the key for both encryption and decryption. At first the image has been divided into eight bit planes and in each bit plane different scan patterns has been used to rearrange the pixel in order to encrypt it.

So for each bit plane there are a separate key to decrypt it. A detail discussion about scan patterns and scan paths has been presented in the next chapter.

CHAPTER 2:

LITERATURE REVIEW

2.1 INTRODUCTION TO SCAN PATTERNS

A scanning of a 2-D array as defined by S.S.Maniccam and N.G.Bourbakis [2] is nothing but an order in which each and every element of that array is accessed only and exactly once. In this report the words scanning, scan patterns, scan paths are used interchangeably. So as an element is processed only once in an array, an (NxN) array will have (NxN)! scanning. Which means an 4x4 2-D array will have (16)! or 20922789888000 scannings. Here in figure 2.1 two different scannings has been shown on a 4x4 array among which one is widely used raster scanning.

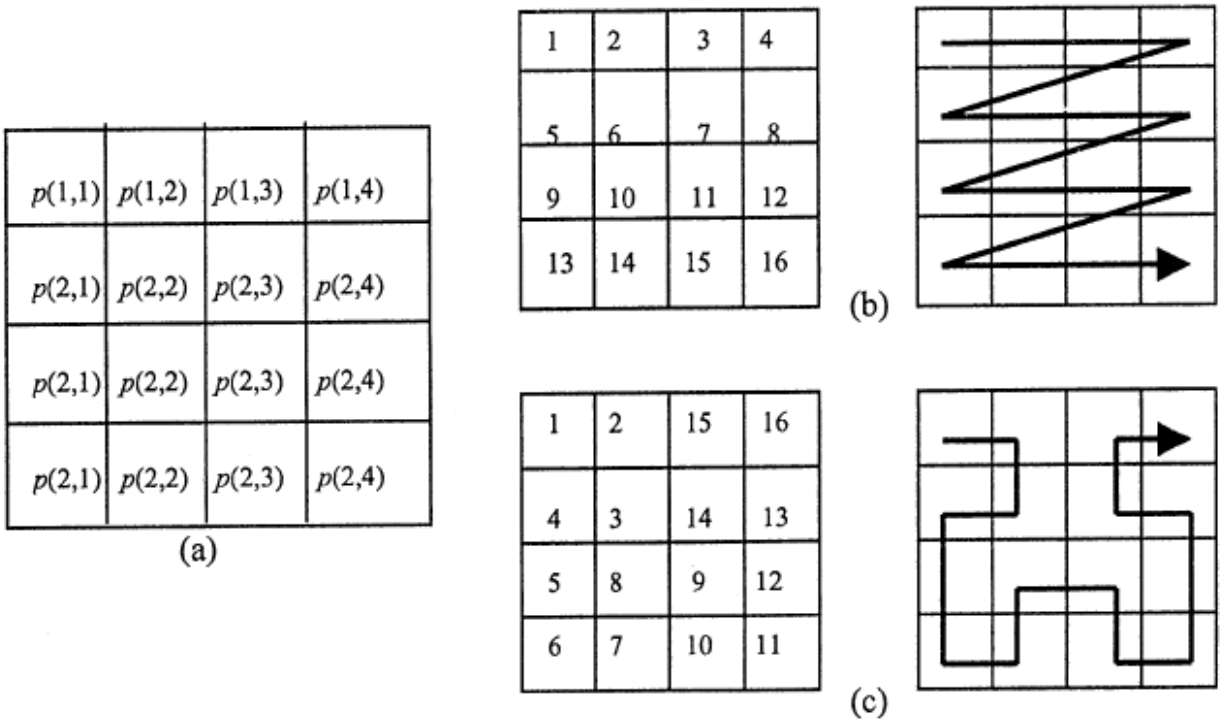


Fig.2.1: (a)an 4x4 array (b)raster scanning (c) another scanning

2.1.1 BASIC INTRODUCTION OF SCAN

The scan is a formal language based methodology which is capable of creating a huge number of scan paths of a 2-D array by accessing its spatial property. There are different

scanning methods based on different application such as simple SCAN, extended SCAN and generalized SCAN, each of which has a specific set of scan patterns.

Each different scannings has its own grammar and a set of basic scan patterns defined. However there are total fifteen scan patterns defined including all the scanning. Each basic scan patterns has a set of transformation and a set of laws to obtain complex scan pattern from basic ones if necessary. The laws for complex scan patterns from basics are defined by the production rules of the grammar of that specific scanning. Below in figure 2.2 all the scan patterns have been shown.

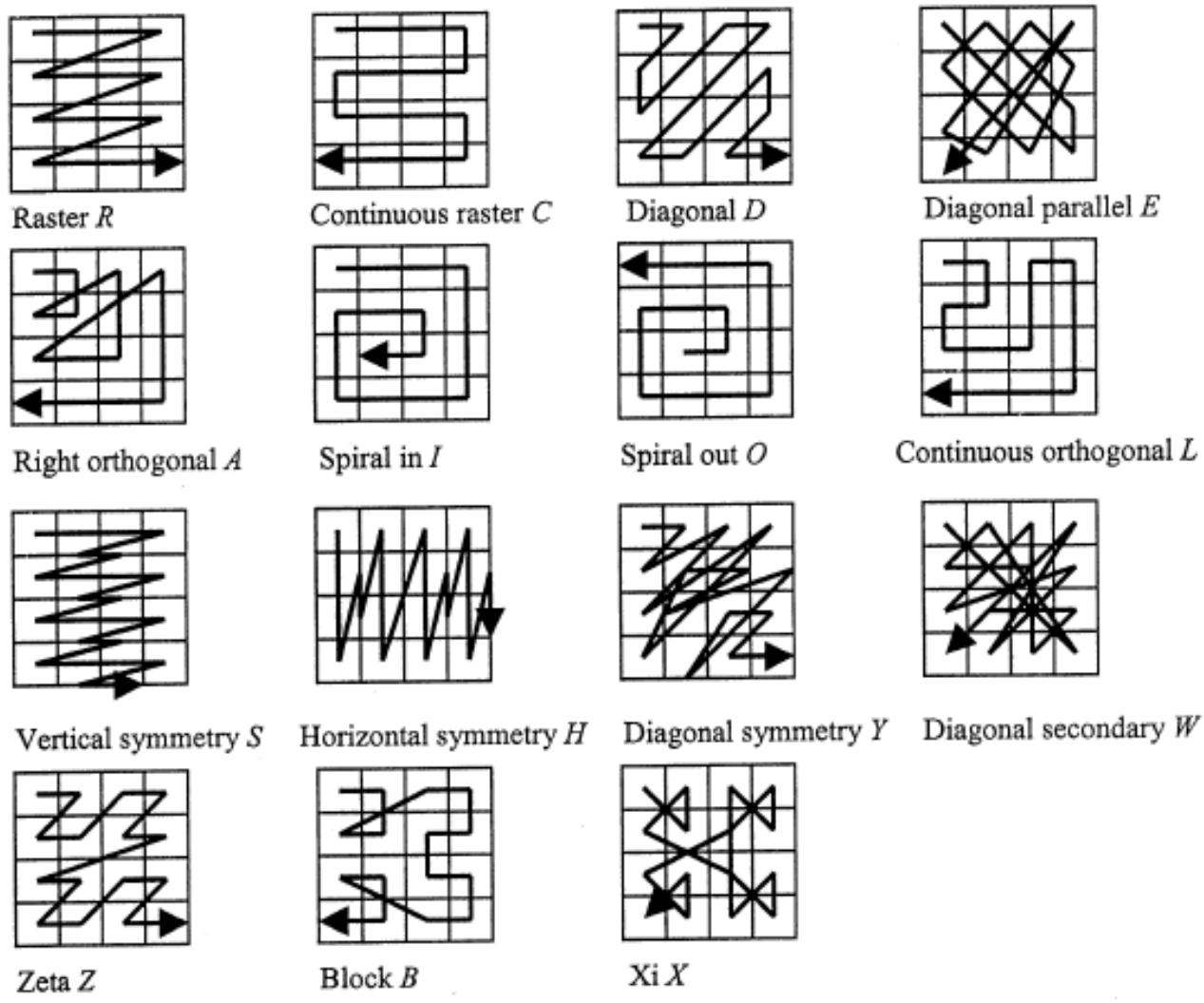


Fig.2.2: basic scan patterns

2.1.2 COMPRESSION AND ENCRYPTION USING SCAN PATTERN

Scanning is used for image compression [11],[9] and image encryption[3],[4],[12] separately earlier. And both compression and encryption using scanning has been proposed by N.G.Bourbakis in ref. [2], But no specific methodology had been provided. Later in ref.[1] both the development and implementation of scanning for lossless image compression and encryption is described by S.S.Maniccam and N.G.Bourbakis.

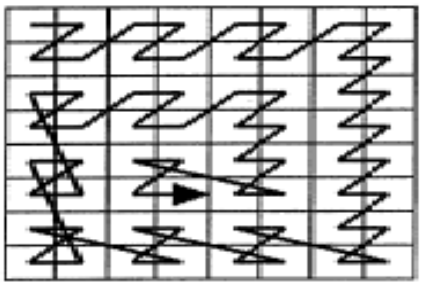
2.2 COMPRESSION AND ENCRYPTION SPECIFIC SCAN

2.2.1 KEY FACTORS OF COMPRESSION AND ENCRYPTION SPECIFIC SCAN

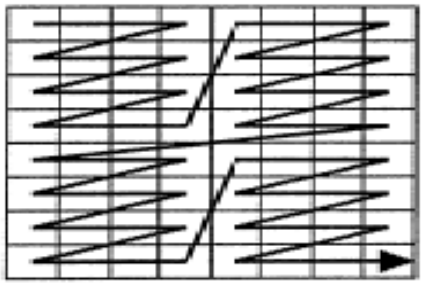
The compression and encryption using scan is applied on binary images. And the bit sequence along the scan path and the bit sequence to represent the scan path together represents encrypted and compressed image. So here is some key factors that should be considered about the sequences representing scan paths –

(a) The scan path should be compact enough so that the bits needed to represent them can be less.
(b) In practice most of the images are non-homogeneous, so they should be scanned using non-homogeneous scan paths, so that the bit sequence will have large number of segments of 0s and 1s. This will lead to fewer bits to encode the sequence. In other words the grammar should be capable of specifying complex scan paths.
(c) There are certain regions in an image which takes more bits to compress it then the original one. Such subregions should be kept in its original form in compressed image.

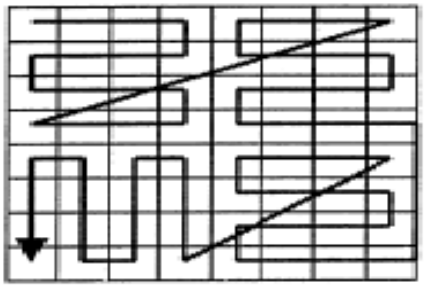
Keeping in mind these factors a generalized scan will be more suitable to preform both compression and encryption, as because though simple SCAN and extended SCAN are compact, but in case of non-homogeneous image these cannot provide non-homogeneous scan paths efficiently. But generalized scannings cannot store image subregions without compression and also it takes large bit sequence to represent. Figure 2.3 depicts simple, extended and generalized scan patterns.



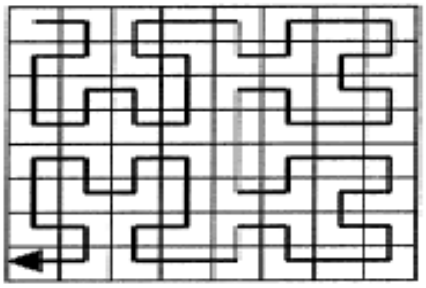
(a) Simple SCAN pattern *I4#Z2*



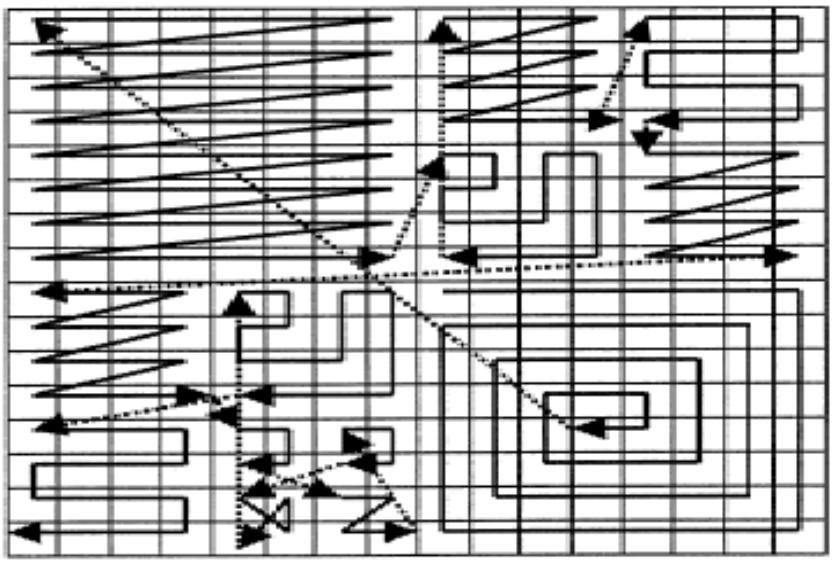
(b) Simple SCAN pattern *R2#R4*



(c) Extended SCAN pattern *Z2(IDEN SYMV SYMV$ROT1 ROT2)*



(d) Extended SCAN pattern *B2(SYMH$ ROT1 IDEN IDEN SYMV$ROT1)#B2 (SYMH$ROT1 IDEN IDEN SYMV$ ROT1)#B2*



(e) Generalized SCAN pattern $A^{0}_{0}(4^{1})@[R^{1}_{2}(4^{3})\#I^{1}_{1}(4^{5})\#B^{0}_{3}(4^{1})@[R^{1}_{2}(4^{2})\#C^{1}_{3}(4^{2}\#R^{1}_{4}(4^{2})\#L^{1}_{1}(4^{2})]\#Z^{0}_{4}(4^{1})@[R^{1}_{1}(4^{2})\#L^{1}_{3}(4^{2})\#C^{1}_{4}(4^{2})\#X^{0}_{2}(4^{1})@[B^{1}_{1}(4^{1})\#Z^{1}_{2}(4^{1})\#B^{1}_{3}(4^{5})\#X^{0}_{4}(4^{1})]]]$

Fig.2.3: (a)(b)simple, (c)(d)extended and (e) generalized scan patterns

2.2.2 BASIC SCAN PATTARN FOR COMPRESSION AND ENCRYPTION SPECIFIC SCAN

The compression and encryption specific scan uses four basic scan patterns, namely

(a) Rasters scan C.

(b) Continuous diagonal D.

(c) Continuous orthogonal O.

(d) Spiral S.

Each of these scan patterns has eight transformations starting from 0 to 7. And the transformations 1,3,5,7 are just the reverse transformations of 0,2,4,6 respectively. As because compression requires less number of bits for long continuous segments of 0s and 1s, the patterns that has been chosen are continuous in nature. Figure 2.4 shows the basic partition patterns for compression and encryption specific scan.

2.2.3 PARTITIONS

As most images needs different kind of scannings for different regions, compression and encryption specific scan allows an image to be divide into four subregions recursively and each of these subregions to be scanned individually. When an image partitioned, the order in which subregions are to be scanned is defined by a partition pattern. There are three partition patterns namely

(a)Letter B

(b)Letter X

(c)Letter Z

Each of these patterns also has eight transformations starting from 0 to 7. And like the basic scan patterns transformations 1,3,5,7 are reverse transformation of 0,2,4,6. Figure 2.5 shows the partition patterns for compression and encryption specific scan.

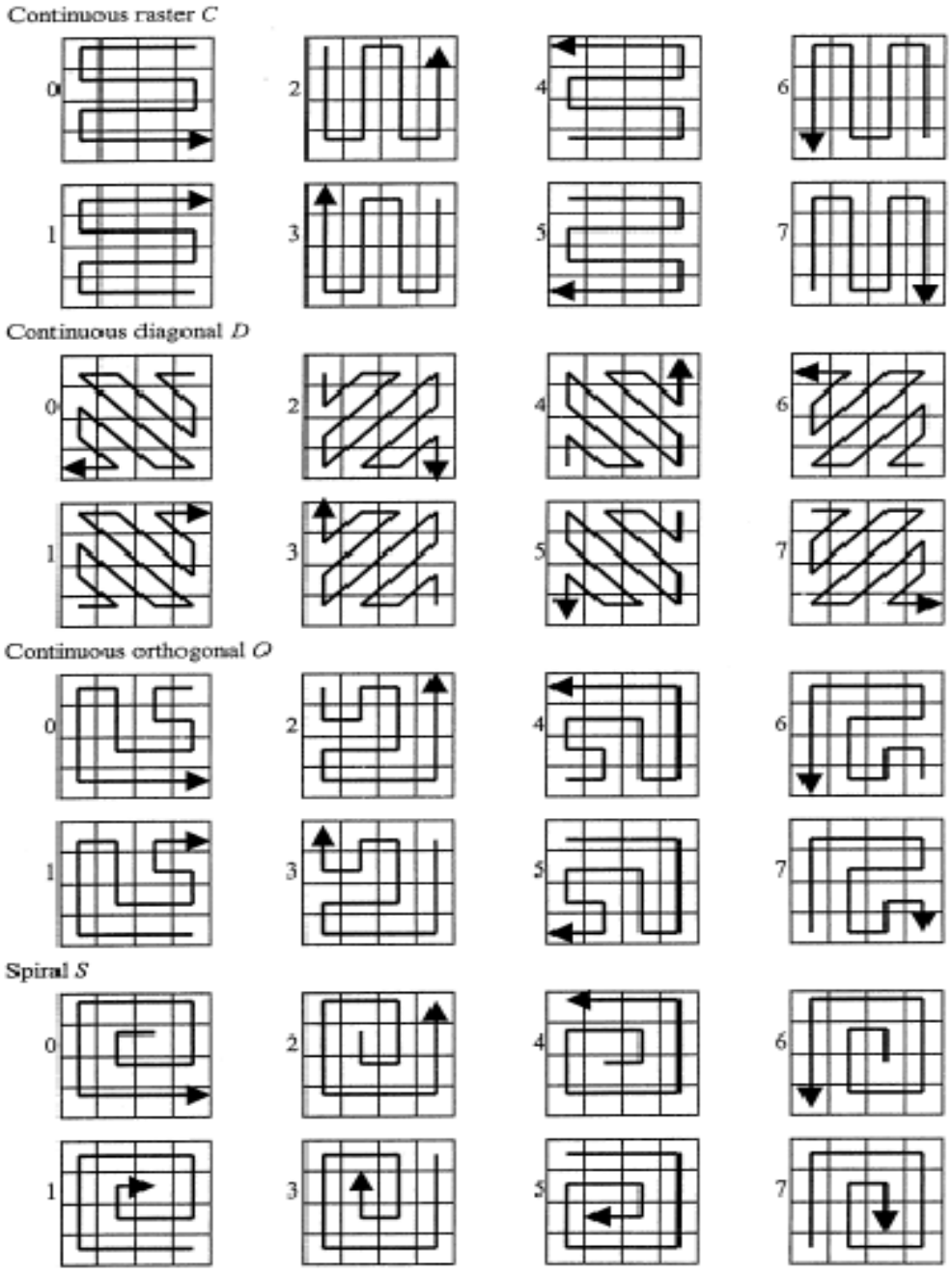


Fig.2.4: Basic scan patterns for compression and encryption specific scan

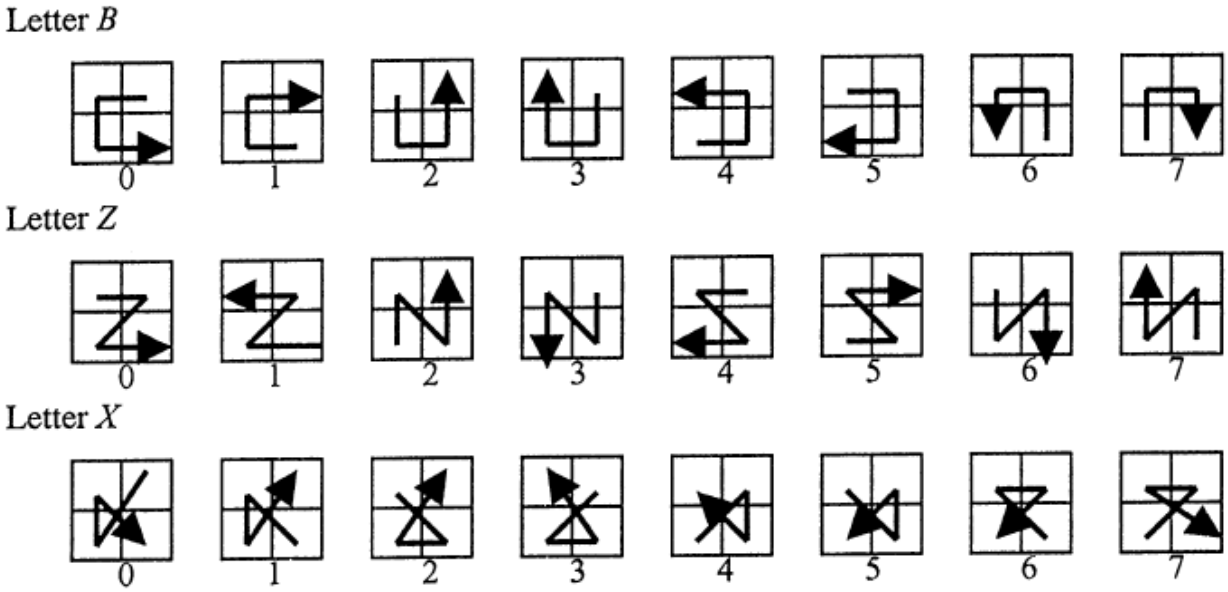


Fig.2.5: Partition pattern

2.2.4 GRAMMAR FOR SCAN PATHS

The compression and encryption specific scan is formally defined by the grammar

$$G = [\Gamma\ \Sigma\ A\ \Pi]$$

Where Γ = non terminal symbols = {A, S, P, I, U, V, T, W};

∑ = terminal symbol = {0, 1};

A = start symbol;

∏ = production rules;

The production rules is given by –

A –S|P|I

S—10UT

P—11VTAAAA

I – 0W

U – 00|01|10|11

V – 00|01|10

T – 000|001|010|011|100|101|110|111

W – Binary strings of length 2^{2n}.

2.2.5 ILLUSTRATION OF THE GRAMMER

A – S|P|I – begin the process by basic scan(S) or partition(P) or storing the image without compression(I).

S – 10UT – here S means scanning a region with basic scan pattern U and transformation T. 10 is the prefix which indicates beginning of basic scanning.

P – 11VTAAAA – refers to partition with partitioning pattern V and transformation T. and the process of partition is scanned in order from left to the right. 11 is the prefix which indicates partition.

I – 0W – stands for storing the image of a region. 0 is the prefix for storing an image region.

U – 00|01|10|11 – it means four of the different scan patterns. 00 is for continuous raster scan C, 01 is for continuous diagonal D, 10 for orthogonal O and 11 for spiral S.

V – 00|01|10 – indicates the partition patterns. 00 for B, 01 for Z and 10 for X.

T – 000|001|010|011|100|101|110|111 – T stands for eight transformations of scanning or partition from 0 to 7 respectively. Here the transformation prefixes are nothing but the binary code of the respective transformation numbers.

W – Stands for storing the original image data without compression. It is a binary bit stream of length $2^{2n.}$

2.2.6 ILLUSTRATION WITH AN EXAMPLE

Now an example has been shown below to illustrate the scan word with the implementation of

compression and encryption specific scan grammar. Figure 2.6 shows a sample scan path and its corresponding scan word with explanation.

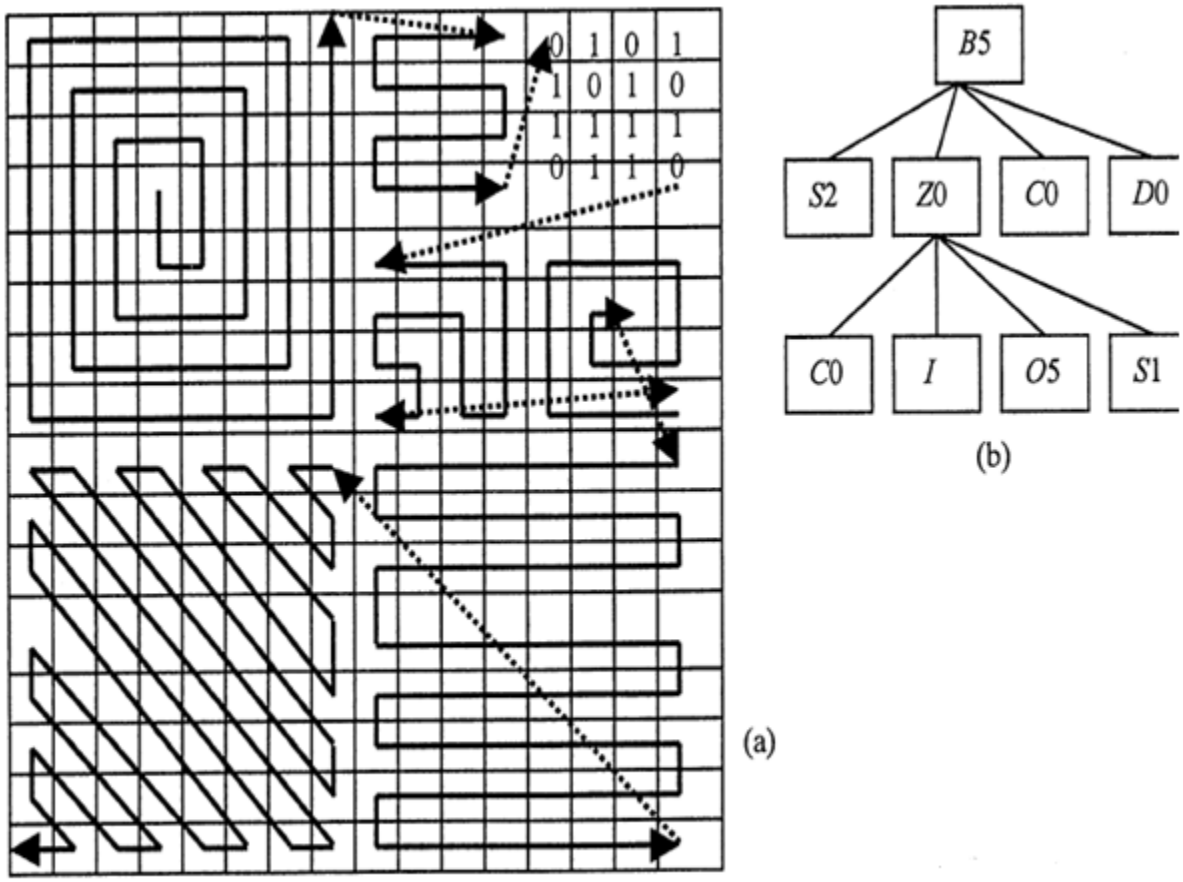


Fig.2.6: (a) sample scanning path of a 16x16 image (b) scan tree for the sample scan path

In the figure shown above there is a region in the image that has not scanned and stored it in the compressed image. In such cases the order in which the bits are stored in compressed image is raster R shown in figure 2.2.

Scan tree shown in figure 2.6(b) is another representation of scan path. It is a top to bottom approach. It begins with a partition pattern. And each partition pattern has four branches going down as a partition pattern divides an image region into four sub regions. As shown in figure 2.6 B5 is the first partition pattern and the four sub regions are scanned with S2, Z0, CO, DO. As there is another partition pattern Z0 four more branches going down from Z0 for scanning its sub

regions and they are C0,I,O0,S1. The scan pattern can also be represented as B5(S2 Z0(C0 I O0 S1)C0 D0). It is nothing but a linear representation of scan tree.

Now forming the scan word from the scan tree –

For B5 – 11 will be prefix as it represents partition of a region. Then 00 will come to represent the partition pattern B. and 101 to represent the transformation 0. So it becomes 1100101.

For S2 – 10 is the prefix as it represents scanning the region with basic scan pattern. S is the scan pattern and is will be represented by 11 and the transformation 2 is replaced by 010. So it is 1011010 for S2.

For Z0 – again 11 will be the prefix for partition of a region. Z will be replaced by 01 and for transformation 0 it is 000. So the scan word for Z0 is 1101000.

For C0 – 10 will be the prefix to initialize the scan of a region. 00 is the code for basic scan pattern C and 0 will be replaced by 000. So the scan word becomes 1000000.

For I – 0 will be the image prefix as a mark of storing the bits of original image. The bits will be scanned in raster R order. So the sequence will become 0 0101101011110110.

For O0 – 10 is prefix for scanning a region. Scan pattern O will be replaced by its corresponding code 11 and transformation 0 is replaced by 000. So the scan word becomes 1011000.

For S1 – 10 is the prefix as it represents scanning the region with basic scan pattern. S is the scan pattern and is will be represented by 11 and the transformation 1 is replaced by 001. So it is 1011001 for S2.

For C0 – 10 will be the prefix to initialize the scan of a region. 00 is the code for basic scan pattern C and 0 will be replaced by 000. So the scan word becomes 1000000.

For D0 – 10 is the prefix as it represents scanning the region with basic scan pattern. D is the scan pattern and is will be represented by 01 and the transformation 0 is replaced by 000. So it is 1001000 for D0.

So putting all these together the scan word for the entire image becomes 11001011011010110 1000100000000101101011110110101010110110011000000100100 0.

2.2.7 COMPRESSION OF IMAGE

A compressed image using compression and encryption specific scan has five components. They are:

(a) Image size,
(b) Scan path that is used for compression
(c) Segments of 0s and 1s.
(d) First bit of scanning path,
(e) Bit stream along the scan path.

Each component is encoded as a 1-D array bit sequence. Then the encoded bits are arranged in specified order as shown in figure 2.7.

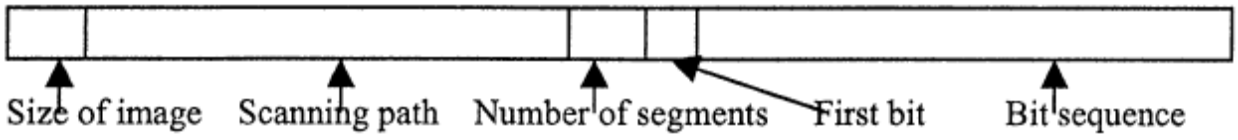


Fig.2.7: components of a compressed image

2.2.8 ENCODING IMAGE SIZE

The methodology first encodes the size of a given image. It assumes that the image is in a size of 2^n x 2^n, and encodes it with (n-3) bits. Here in this work n varies from 2 to 9. However it can be extended into larger images.

2.2.9 ENCODING SCAN PATH

The algorithm for compression and encryption specific scan first find a good scan path using which an image can be represented with minimum number of bits. After such scan path is determined the grammar is applied and the bit stream is opted for the corresponding scan word. As an example if the scan path opted by the algorithm is Z3(C1S5C2D7), then its corresponding encoded bit stream will be 1101011100000110 11101100001010 01111.

2.2.10 ENCODING SEGMENTS AND FIRST BIT

The next component of a compressed image is the first bit of the scan path and after that it is the number of segments present in the compressed image. The first bit will be 1 or 0 for a scan path and it is encoded as it is using 1 bit. The segment number on the other hand is represented by 2n bits for 2^n x 2^n image size. For example if there is an image (8x8) having bit sequence along the scan path is 1111110000000000000110000111000000000111111100000 0011111111111000 then the segment size will be encoded as 001010 as there is 10 segments and n=3. So it is encoded using six bits.

2.2.11 ENCODING BIT SEQUENCE

After the compression rule determines the scanning path, the bit sequence on the scanning path is determined. The bit sequence is then encoded victimization a modified run length encryption. During this run length encryption, a bit segment of size n is encoded as binary type of (n- lower limit of n) using the quantity of bits and prefix shown in Table one. All encoded segments are then appended together. The advantage is that little phase sizes which occur additional usually are encoded using fewer bits, and large phase sizes that occur less usually are encoded using number enough variety of bits.

2.2.12 ENCRYPTION AND DECRYPTION

The compression and encryption algorithm first do the compression and after that another scan path is applied to the compressed image. This is for encryption purpose. The scan path for encryption is kept secret as the key which is used in both encryption and decryption. The key used at the both end are same, that's why this is called symmetric key encryption. The key should be known to the receiver prior to the decryption process otherwise decryption cannot be done.

CHAPTER 3:

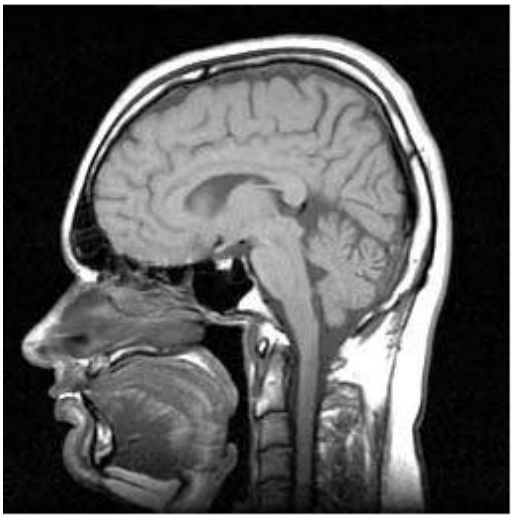
WORK DONE

3.1 SAMPLE IMAGES

In the experimental scenario for image compression and encryption using scan path four different images has been taken each of which has different intensity variations. These images are cameraman.tiff, lena.png, pepper.jpg, MRI_head_side.jpg. In figure 3.1 sample images has been shown.

(a)

(b)



(c)

(d)

Fig.3.1: sample images,(a)cameraman.tif, (b) pepper.jpg (c)MRI_head_side.jpg, (d)lena. jpg

3.2 OPERATIONS INVOLVED

Here the images are encrypted first and then compressed using run-length coding. And both the encrypting scan path and compression scan path are kept secret. Doing this the security of the encrypted and compressed image is enhanced. The chapter is divided into two parts as (1) encryption and compression and (2) decompression and decryption.

3.2.1 ENCRYPTION AND COMPRESSION

The methodology that has been described in the previous chapter is slightly modified in the experimental algorithm for encrypting and compressing a grayscale image. Here the encryption has done using the concept of symmetric key cryptography. But there are two key used to provide a good security to the image at different stages in the algorithm. The operations that are involved in encrypting and compressing an image are shown in the figure 3.3. The operations involved in encryption and compression is described below.

3.2.1.1 OPERATION I: BIT PLANE SLICING

Taking the sample gray scale image the first operation that is done is bit plane slicing[10]. Bit plane slicing is a method of dividing an image into eight different planes of 1s and 0s. The unit element of any digital image is called pixel and it's finite in number for a specific image. And every pixel has got some value. In case of grayscale image the value is known as intensity level and it ranges from 0 to 255. And each pixel value is represented by 8 bits, starting from MSB (most significant bit) to LSB (least significant bit). Bit plane slicing is actually a process of forming a plane of 1s and 0s by taking all the bits of same position of all the pixels. For example

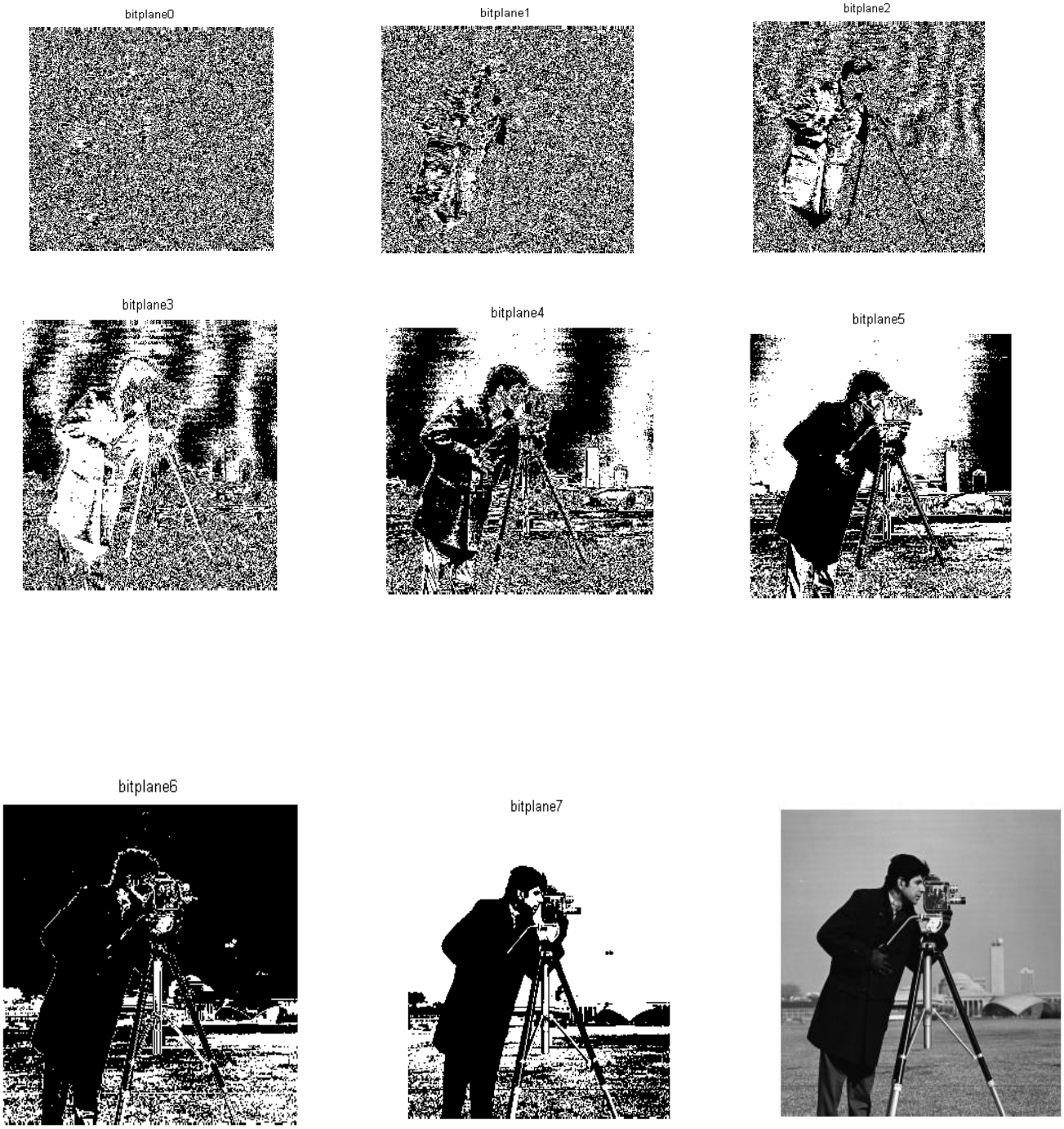


Fig.3.2: bit plane from 0 to 7 and the original grayscale image ‘cameraman.tif’

3.2.1.2 OPERATION II: SPECIFING SCAN PATH

There are four basic scan patterns and each of which has 8 transformations used in this encryption and compression algorithm. So using the combination of these 32 scan patterns the optimum or good scan path has to be determined. Also the partition pattern which are letter B, letter z and letter x with 8 transformations each have to be chosen carefully to obtain minimum number of bits to represent the entire image. At first all 32 scan patterns and the partition pattern has been defined. At the time of encryption a random combination of scan pattern and partition pattern is been applied on the bit plane. After that the compression is done and it is compared with a threshold value. The threshold value is the compression ratio to determine that whether or not the image has been compressed enough. The threshold values is given below in table.1 and these values are predetermined empirically by experiments [1].

Image region size	Threshold values
8x8	1.2
16x16	5
32x32	10
64x64	20
128x128	30
256x256	50
512x512	100

Table.3.1: region sizes and threshold values

If the combination of the scan patterns and partition patterns that are chosen randomly gives a compression ratio less then threshold then the process repeats and goes on until a scan path is not determined which gives compression ratio more than the threshold value. Here as mentioned that the partition can be of any size, but in this work the partition has maintained to 8x8 because of

the experimental checking. After the compression another scan path chosen randomly to rearrange the bit stream of encrypted and compressed image to enhance the security.

3.2.1.3 OPERATION III: COMPRESSION

After a scan path is determined randomly and applied to the bit plane, now the next step is to perform compression to the encrypted bit plane. First of all the entire bit plane is converted into an array of bit stream and then a run length encoding is applied to it. run length coding that is used here is the conventional run length coding. No modification is done as it is mentioned in the paper[1].

Run length coding is a simple algorithm which is used to compress a data set having subsequent repetition of same data. By compressing a data set a code is achieved. The basic idea is to replace the repetition of a data by a counter which indicates the number of repetitions occurred. Here in this work run length encoding is used to encode the binary bit stream. The encoded data is a matrix. Where the first row contains the value (0 or 1) and the second row contains the run length of the corresponding value.

After the compression is done the compression ratio is determined and compared with the threshold value given in table.3.1. If the compression ratio is above the threshold then the compression is done. But in case of a compression ratio less than the threshold the scan path that is applied is rejected and a new scan path is applied and then again it is encoded using run length encoding. The loop continuous for all bit planes.

3.2.1.4 OPERATION IV: ENCRYPTION

Encryption is done twice in this algorithm in order to achieve a higher rate of security and to get a higher compression ratio as well. The first phase is to retain the scan path secret using

which the compression is done. This is key 1 and after the compression is done another scan path is applied to shuffle the bit stream once again and the scan path is retained secret. This scan path is applied after merging all the compressed bit planes. This is key 2. Both the keys should be known by the receiver in order to decrypt and decompress the received image. As the keys used at both ends are same and should be known by the receiver prior to the decryption and decompression algorithm is applied, this is known as symmetric key cryptography.

3.2.1.4 OPERATION V:OBTAINING ENCRYPTED AND COMPRESSED IMAGE

After encryption and compression is done all the bit plans merged to get the compressed and encrypted image. After marging the bit planes a suffle is done using a scan path as mentioned earlier, to obtain higher security and robustness against external attacks.

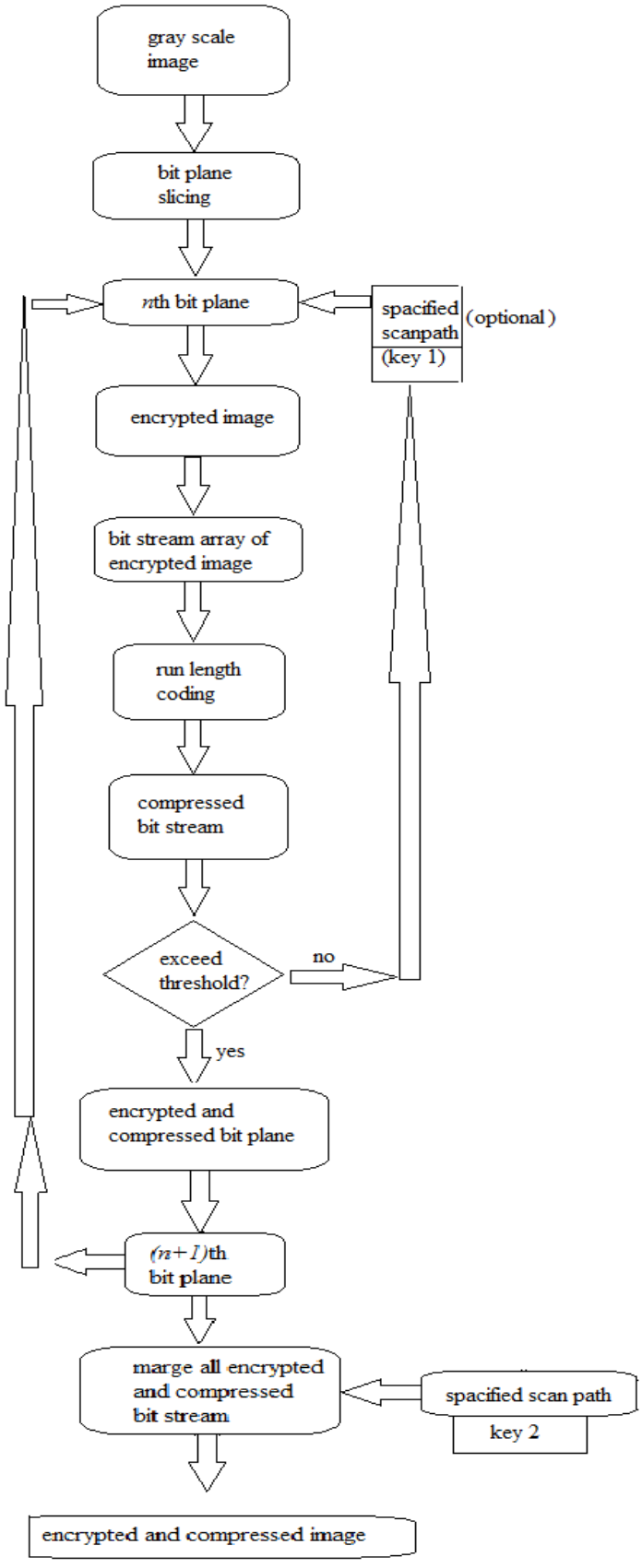


Fig.3.3: encryption and compression

3.2.2 DECOMPRESSION AND DECRYPTION

In case of decompression and decryption the involved operations has been shown in figure 3.4 and a detailed discussion is followed below.

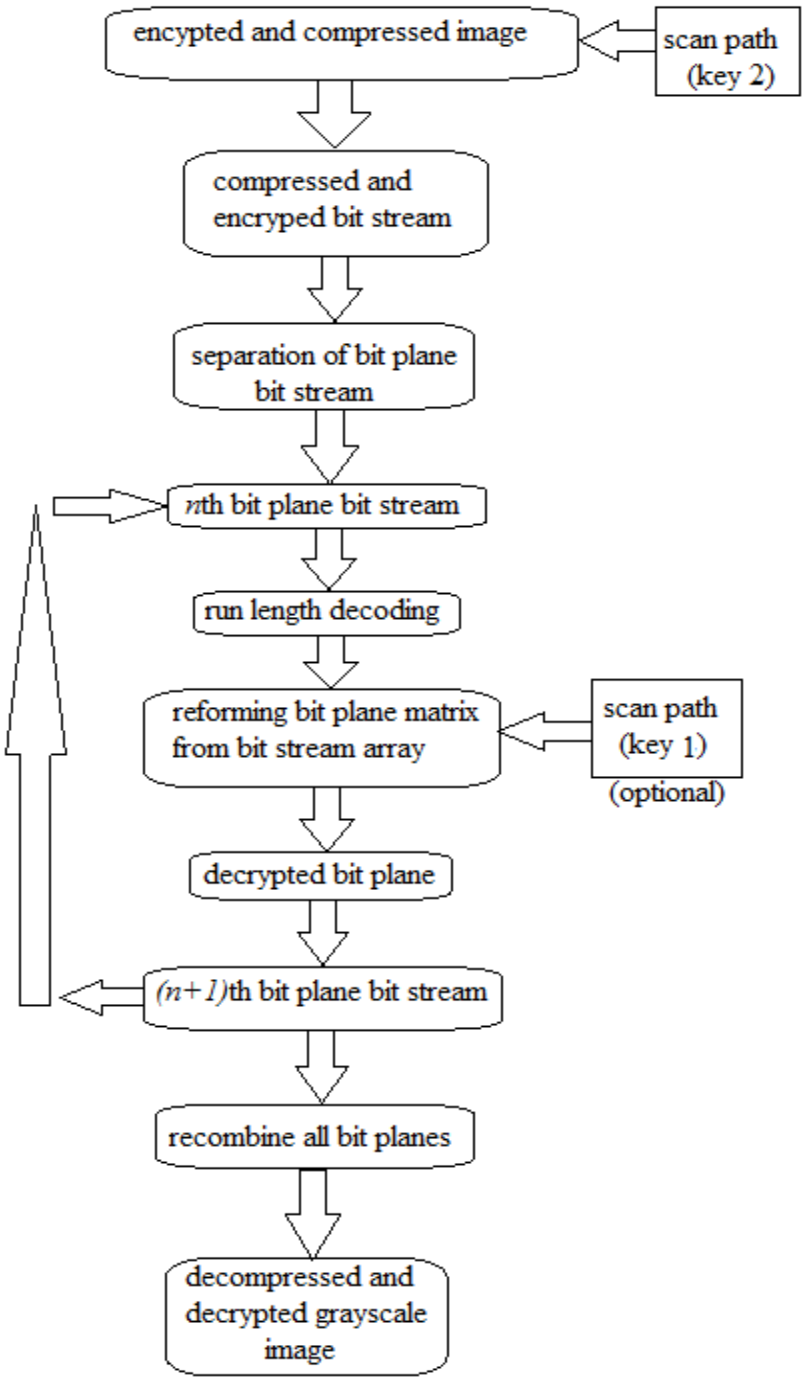


Fig 3.3: decompression and decryption

3.2.2.1 OPERATION I: DECRYPTION OF ENCRYPTED AND COMPRESSED GRAYSCALE IMAGE

At first the encrypted and compressed is decrypted by key 2, which was earlier applied on the bit stream of combined bit plane bit stream. After the scan path is applied the resultant bit stream is the combination of 8 bit planes which are still compressed and encrypted in form. Now bit plane bit streams are divided and decompression and encryption is performed with each different bit plane bit stream.

3.2.2.2 OPERATION II: DECOMPRESSION

After the separation of bit plane bit stream, run length decoding is performed. In case of run length decoding, it takes the value and repeats it according to its run length which was encoded earlier. After run length decoding a bit stream of 1s and 0s is obtained. This is the bit stream of the bit plane but still in encrypted form.

3.2.2.3 OPERATION III: DECRYPTION AND FORMING BACK GRAYSCALE IMAGE

After getting back the bit stream of the same size of the bit plane, first it is brought back to a matrix form. Then key 1 is applied to it. key 1 is the scan path which is used for image compression with a compression ratio above threshold value. After decryption is done the bit plane is retrieved. This process is applied to each bit plane and after getting all the bit planes, all 8 planes are recombined to get back the original image.

CHAPTER 4:

RESULTS AND DISCUSSION

4.1 EXPERIMENTAL RESULTS

The results opted after applying the algorithm has been shown below. Four different sample images (widely used) are taken which has different intensity variations. The methodology works on the binary images, so each image has been scaled into its corresponding bit planes and then the algorithm applied on it. Figure 4.1(a) to (h) shows the compression and encryption done on each bit plane on the sample image ‘cameraman.tif’.

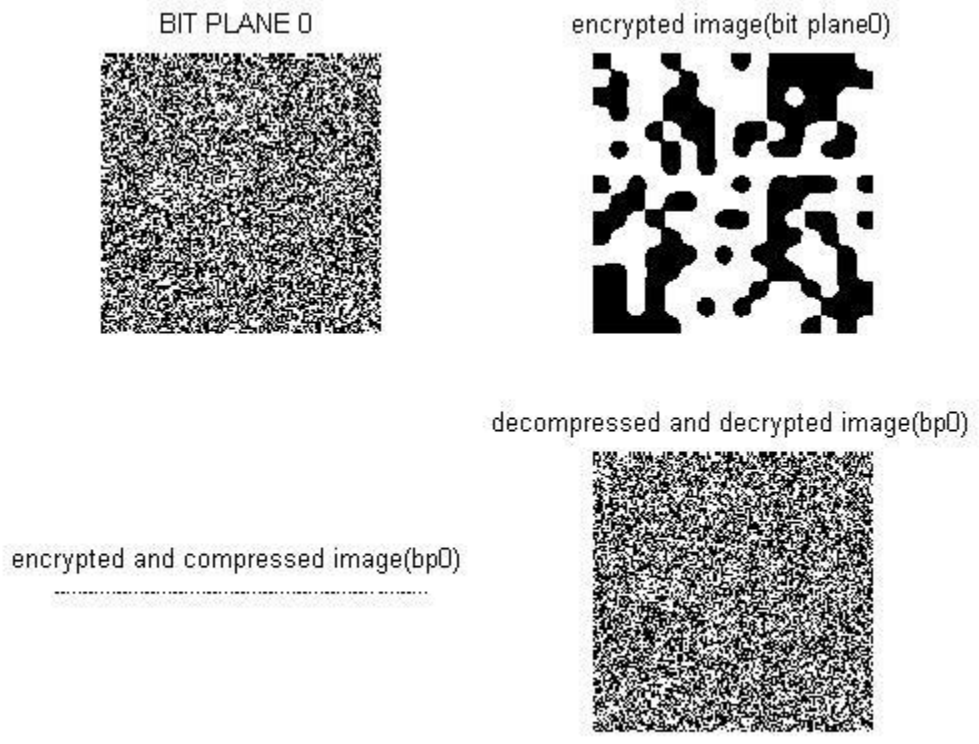


Fig.4.1 (a) bit plane 0 for 'cameraman.tif'

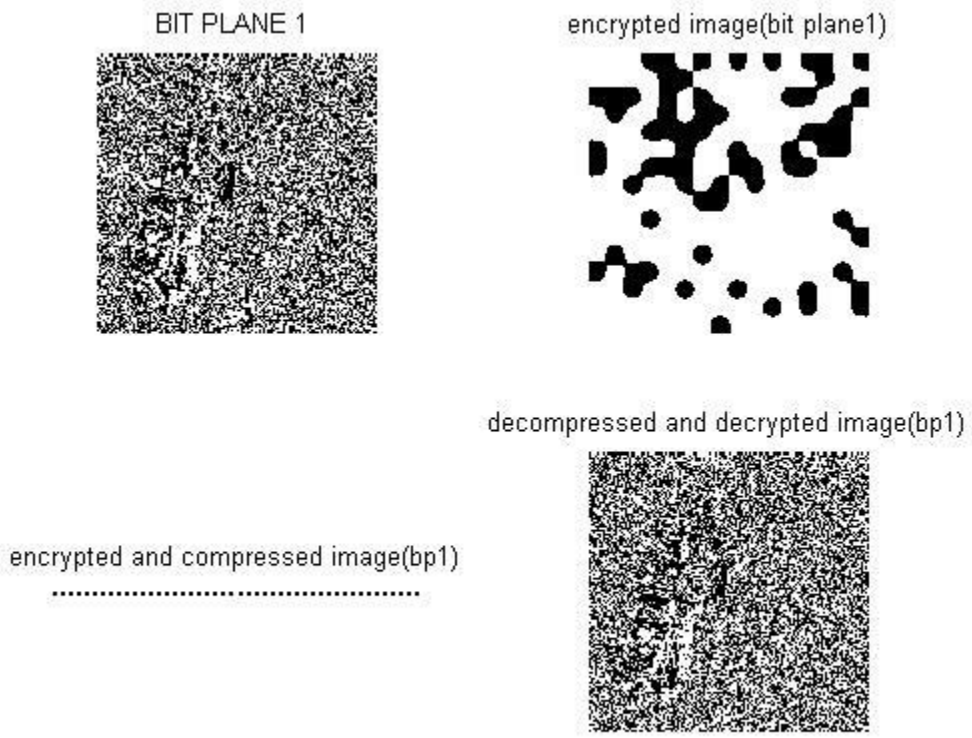


Fig.4.1 (b) bit plane 1 for 'cameraman.tif

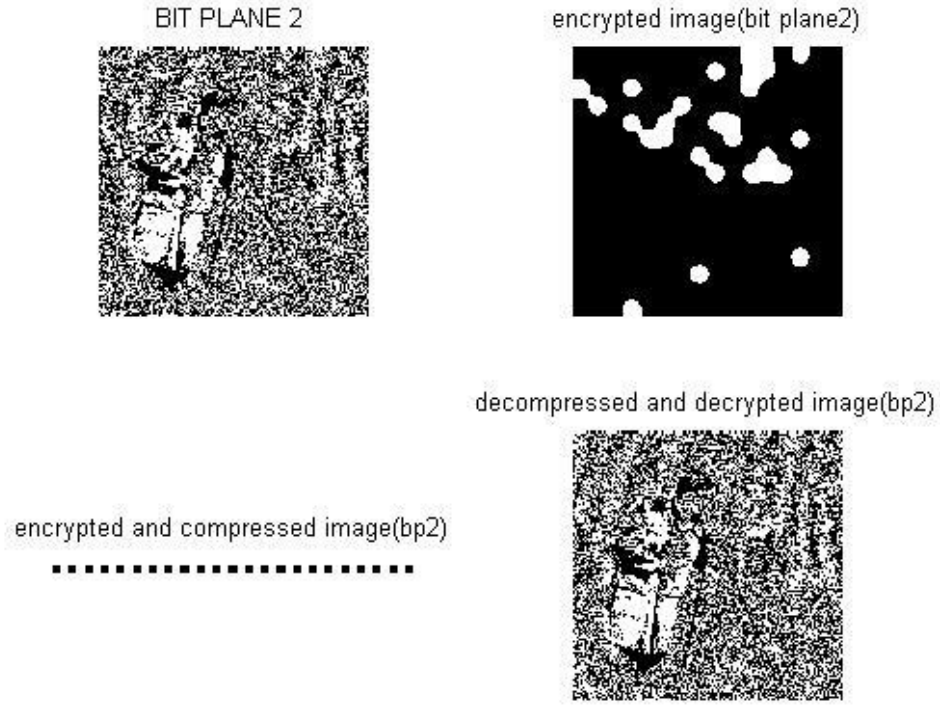


Fig.4.1 (c) bit plane 2 for 'cameraman.tif

BIT PLANE 3

encrypted image(bit plane3)

decompressed and decrypted image(bp3)

encrypted and compressed image(bp3)

Fig.4.1 (d) bit plane 3 for 'cameraman.tif

BIT PLANE 4

encrypted image(bit plane4)

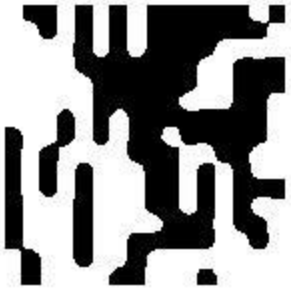
decompressed and decrypted image(bp4)

encrypted and compressed image(bp4)

Fig.4.1 (e) bit plane 4 for 'cameraman.tif

BIT PLANE 5

encrypted image(bit plane5)



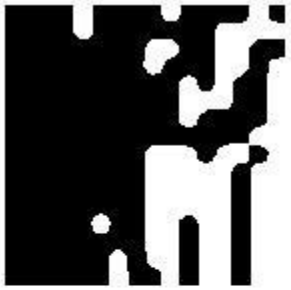
decompressed and decrypted image(bp5)

encrypted and compressed image(bp5)

Fig.4.1 (f) bit plane 5 for 'cameraman.tif'

BIT PLANE 6

encrypted image(bit plane6)



decompressed and decrypted image(bp6)

encrypted and compressed image(bp6)

Fig.4.1 (g) bit plane 6 for 'cameraman.tif'

BIT PLANE 7

encrypted image(bit plane7)

decompressed and decrypted image(bp7)

encrypted and compressed image(bp7)

Fig.4.1 (g) bit plane 7 for 'cameraman.tif'

original grayscale image

compressed and encrypted grayscale image

retrived grayscale image

Fig.4.1 (h) grayscale image and its correspondig encrypted and compressed image and retrieved image

Here in the table 4.1 below the corresponding compression ratio for each bit plane has been shown. Compression ratio is described as:

$$CR = \frac{total\ number\ of\ bits\ in\ the\ original\ image}{(total\ number\ of\ bits\ in\ compressed\ image)}$$

Bit plane	Original size	Compressed size	Compression ratio
0	256*256	2*27072	1.2108
1	256*256	2*27264	1.2022
2	256*256	2*16128	2.0324
3	256*256	2*15872	2.0651
4	256*256	2*22272	1.4717
5	256*256	2*21248	1.5426
6	256*256	2*15360	2.1340
7	256*256	2*15872	2.0651
Grayscale image	256*256*8	2*168192	1.5586

Table 4.1: compression ratio for different bit plane for the image 'cameraman.tif'

For other sample grayscale images only the grayscale image, its corresponding compressed and encrypted images and retrieved image has been shown.

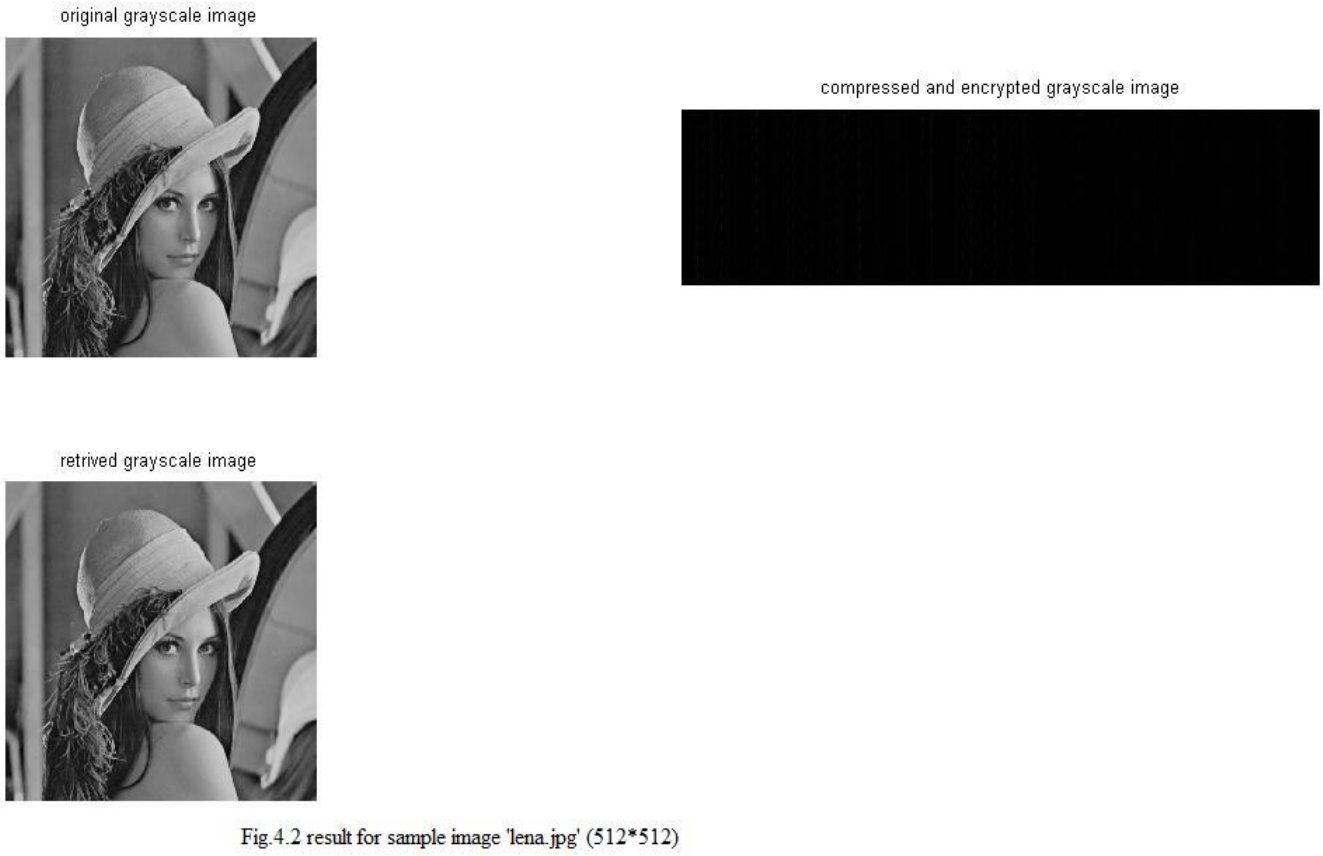


Fig.4.2 result for sample image 'lena.jpg' (512*512)

Corresponding bit plane compression ratio for sample image ‘lena.jpg’ has been shown in table 4.2 below

Bit plane	Original size	Compressed size	Compression ratio
0	512*512	2*108992	1.2026
1	512*512	2*108289	1.2104
2	512*512	2*109184	1.2005
3	512*512	2*78848	1.6623
4	512*512	2*107393	1.2205
5	512*512	2*76801	1.7067
6	512*512	2*94208	1.3913
7	512*512	2*78785	1.6623
Grayscale image	512*512*8	2*745204	1.4071

Table 4.2: compression ratio for different bit plane for the image ‘lena.jpg’

The resulting images of sample image ‘pepper.jpg’ after applying the algorithm has been shown below in figure 4.3 and the statistics of each bit plane is given in table 4.3.

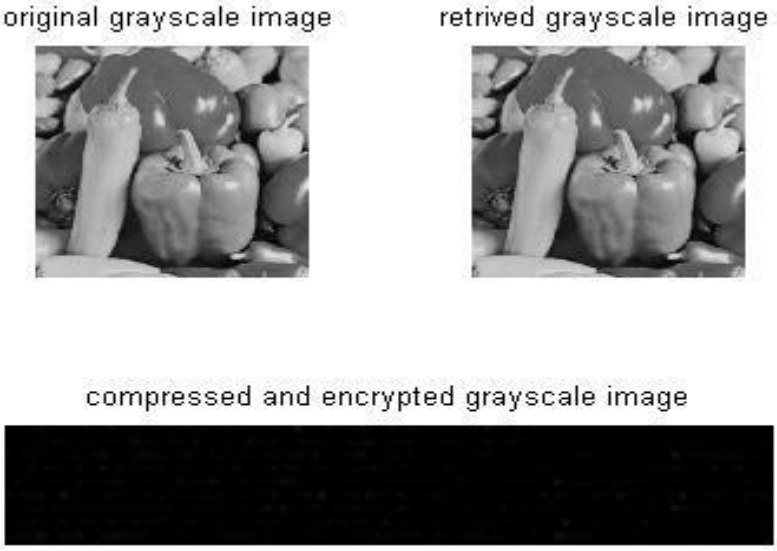


Fig.4.3: result for sample image 'pepper.jpg'

Bit plane	Original size	Compressed size	Compression ratio
0	256*256	2*16991	1.2140
1	256*256	2*27264	1.2019
2	256*256	2*27168	1.2061
3	256*256	2*23713	1.3819
4	256*256	2*22784	1.4382
5	256*256	2*25855	1.2673
6	256*256	2*22784	1.4382
7	256*256	2*23552	1.3913
Grayscale image	256*256*8	2*198986	1.3174

Table 4.3: compression ratio for different bit plane for the image ‘pepper.jpg’

Here is another sample image which is a medical image and its corresponding outputs and the compression statistics has been shown below in figure 4.4 and table 4.4 respectively.

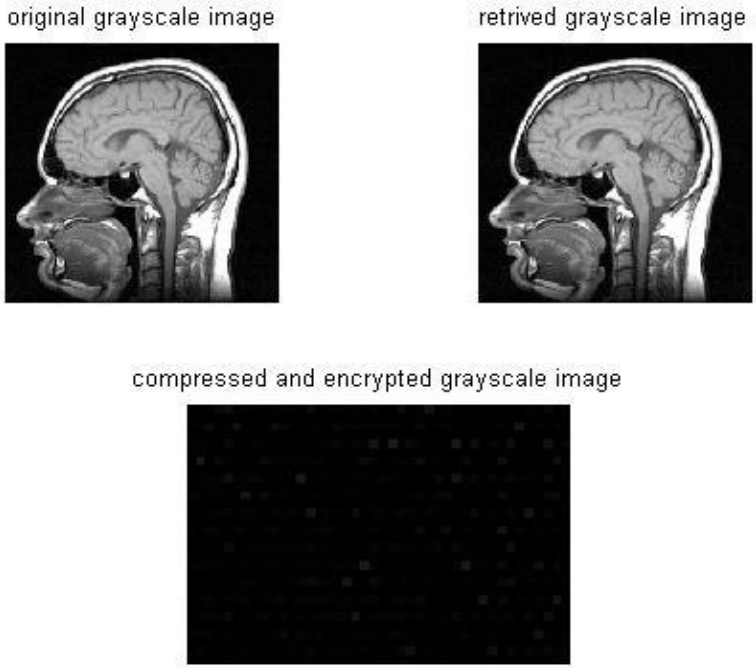


Fig 4.4: Result for sample image 'MRI_head_side.jpg'

Bit plane	Original size	Compressed size	Compression ratio
0	256*256	2*17645	1.8551
1	256*256	2*17920	1.8286
2	256*256	2*20736	1.5802
3	256*256	2*19703	1.6631
4	256*256	2*17152	1.9104
5	256*256	2*20736	1.5802
6	256*256	2*22784	1.4382
7	256*256	2*19712	1.6623
Grayscale image	256*256*8	2*161280	1.6254

Table 4.4: compression ratio for different bit plane for the image 'MRI_head_side.jpg'

From the results shown above it is certain that this algorithm works better for the images which has more homogeneous regions. But all the above process has been done using the conventional method of keeping only one key for encryption. So the scan path which is used for compression is given with its corresponding bit planes as shown in figure 2.7. But if higher security and higher compression ratio is needed than keeping both the compression scan path and encryption scan path secret is the appropriate choice. It has been also tested and a comparison is shown between the compression ratio for both case one key encryption and two key encryption has been shown below in table 4.5.

IMAGE	COMPRESSION RATIO	
	Single key encryption	Double key encryption
Cameraman.tif	1.5586	2.0687
Lena.jpg	1.4071	1.7067
Pepper.jpg	1.3174	1.4222
MRI_head_side.jpg	1.6254	2.1880

Table 4.5 comparison of compression ratio between single key and double key encryption

As table 4.5 depicts, it is quite clear that double key encryption method not only allows higher security against cryptanalysis but also provides better compression ratio as compared to single key encryption. This is because the scan paths that are used for the compression is coded and the bit sequence is patched with the image in case of single key encryption. But in double key encryption the scan paths for compression are used as a key. So there is no need to provide the bit sequence of it along with the image. So there is less number of bits in encrypted and compressed image for double key encryption method.

4.2 ADVANTAGES AND DISADVANTAGES

The methodology described here has an upper hand to the existing image compression or encryption methods because none of them can perform both compression and encryption together. But it also has some limitations. Below the advantages and dis advantages are discussed.

4.2.1 ADVANTAGES

(1) The main advantage that has been said quite a few times earlier is this methodology can perform both compression and encryption at the same time.

(2) The compression done here is lossless in nature. But lossy compression can also be achieved using the elimination of the LSB bit plane as it carries least information about an image and is ignorable.

(3) Encryption can be done using single key and double key according to the demand of security and compression required.

4.2.2 DISADVANTAGES

(1) This method works on binary images. So direct implementation to the intensity level is not possible.

(2) As it uses run length coding for compression quick variations of 1s and 0s can have an adverse effect. So this works better for images having more homogeneous regions.

(3) For grayscale image it has to split the image into 8 bit planes and run compression and encryption for each plane, so the time consumed is higher than the other compression schemes.

(4) Double key encryption gives better security and compression ratio, but as scan path for each bit plane is different for compression the user have to have the access nine keys (eight scan path for compression and one scan path for encryption) to decrypt and decompress the whole image.

CHAPTER 5:

FUTURE WORK AND CONCLUSION

The simultaneous lossless compression and encryption makes this algorithm very useful in the field of medical image processing, multimedia applications, military applications etc. The compression achieved in the experimental results has been simulated using MATLAB R2012a. The compression ratio given by the algorithm is not optimum. There can be other possible combination of scan paths which can provide more efficient compression.

Future work includes a better way to find the scan path so that it can be assured that highest compression ratio is achieved. It also includes the modification of the compression method so that it can be applied on the intensity level for grayscale image directly, doing this compression time can be minimized and the correlations between the pixels can be exploiting better. The colour images can also be compressed using grayscale compression on each red, green and blue component or by directly applying it on the 24-bit colour value. Another thing that needs attention is in case of double key encryption the compression keys are eight in number. So it is a tough job to remember the keys and the number will increase for colour images. so for double key encryption the number of keys have to be reduced.

REFERENCES:

[1] Lossless image compression and encryption using SCAN, S.S. Maniccam, N.G. Bourbakis Pattern Recognition**,** Elsevier, Volume 34, Issue 6, June 2001, Pages 1229–1245

[2] SCAN Based Lossless Image Compression and Encryption S. S. Maniccam, N. G. Bourbakis, Binghamton University, Dept. EE, Image-Video-Machine Vision Lab, Binghamton NY 13902, U.S.A. Technical University of Crete, Dept. ECE, Chania 731 00, Crete, Greece

[3] Data-image-video encryption, Ming Yang ; Bourbakis, N. ; Shujun Li, Potentials, IEEE (Volume:23 , Issue: 3), Aug.-Sept. 2004, pages – 28-34.

[4] Image Encryption and Decryption Using SCAN Methodology Chao-Shen Chen ; Rong-Jian Chen Parallel and Distributed Computing, Applications and Technologies, 2006. PDCAT '06. Seventh International Conference on Digital Object Identifier: 10.1109/PDCAT.2006.71 Publication Year: 2006 , Page(s): 61 – 66

[5] An Introduction to Image Compression, Wei-Yi Wei, Graduate Institute of Communication Engineering National Taiwan University, Taipei, Taiwan, ROC

[6] Security Engineering: A Guide to Building Dependable Distributed Systems, Book by Ross Anderson Published: March 2001

[7] Lossless Image Compression, by B. C. Vemuri , S. Sahni , F. Chen , C. Kapoor , C. Leonard , J. Fitzsimmons

[8] N. Bourbakis, Image data compression encryption using G-SCAN patterns, IEEE Conference on SMC, October 1997, pp. 1117-1120.

[9] N. Bourbakis, C. Alexopoulos, Picture data compression using SCANpatterns, SPIE Conference on Electronic Imaging, February 1993.

[10] G. Drost, SCAN based lossless image compression application specific integrated circuit, Masters Thesis, SUNY Binghamton, 1998.

[11] C. Alexopoulos, N. Bourbakis, N. Ioannou, Image encryption method using a class of fractals, J. Electron. Imaging 4 (3) (1995) page - 251-259.

[12] A Password-Based Key Establishment Protocol wit Symmetric Key Cryptography ; Erguler, I.,Anarim,E., Networking and Communications, 2008. WIMOB '08. IEEE International Conference on Wireless and Mobile Computing, Digital Object Identifier: 10.1109/WiMob.2008.112 Publication Year: 2008 , Page(s): 543 – 548

[13] The comparisons between public key and symmetric key cryptography in protecting storage systems Lanxiang Chen ; Shuming Zhou Computer Application and System Modeling (ICCASM), 2010 International Conference on Volume: 4 Digital Object Identifier: 10.1109/ICCASM.2010.5620632 Publication Year: 2010 , Page(s): V4-494 - V4-502

[14] Digital image processing using MATLAB ; by Rafael C. Gonzalez , Richard E. Woods , Steven L. Eddins, December 26, 2003

[15] Security Engineering: A Guide to Building Dependable Distributed Systems; Ross Anderson, 2nd edition, March 2001